IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	09/576,516
Confirm. No.:	4301
Inventor:	Xin Qiu et al.
Filing Date:	May 23, 2000
Title:	Secure Control of Security Mode
Examiner:	Pyzocha, Michael J.
Art Unit:	2137
Atty. Docket No.:	D02301

Mail Stop Appeal
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

In response to the Rejection mailed on April 26, 2006, please enter this Appeal Brief. The Notice of Appeal was filed on October 26, 2006. A Petition for a One (1) Month Extension of Time is included herewith.

(I) Real Party in Interest

General Instrument Corporation, a wholly owned subsidiary of Motorola, Inc., is the real party in interest.

(II) Related Appeals and Interferences

There are no known related appeals or interferences.

(III) Status of the Claims

Claims 21-32 are cancelled.

Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,602,916 to Grube et al. in view of U.S. Patent No. 5,930,361 to Hayashi et al.

Applicant appeals all pending claims 1-20.

(IV) Status of Amendments

The only amendment after the Rejection mailed on April 26, 2006 is the one that is being submitted concurrently herewith. This amendment corrects a minor informality in claim 12 and cancels claims 21-26 and 28- 32. Applicant believes this amendment should be entered as it materially reduces the issues on appeal.

(V) Summary of the Claimed Subject Matter

In general, the invention relates to a method for transmitting and receiving data using at least two levels of security. Specification, page 1, lines 20-25. Thus, a person

could transmit a low level security message using a low level of security encryption or authorization and then transmit a second message have a higher level of security encryption or authorization. Id. The method also allows for change from one level of security to the other in such a way as to minimize threats from an attacker. Specification, page 2, lines 4-13.

Claim 1 is a method for providing varying levels of security in a data processing system. Specification, page 1, lines 20-25. The method comprises receiving information that a first indication that instructs the system to operate at a higher level of security. See FIG. 1a, block 104 and the specification, page 3, lines 15-19. The method also comprises receiving further information that includes a second indicator for instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator. FIG. 1a, block 124 and the specification, page 4, line 33 – page 5, line 5. The method also comprises preventing operation at the lower level of security until a decrease in the security levels is indicated by said second indicator while continuing operation of the data processing system. FIG. 1b, blocks 140 and 144 and the specification, page 6, lines 15-17.

Claim 20 is a method for providing a secure transition between a high level of security and a low level of security in a data processing system. Specification, page 1, lines 20-25. The method comprises receiving information that includes a first security message that causes the processing system to operate at the higher level of security. See FIG. 1a, block 104 and the specification, page 3, lines 15-19. The method also continues operating the data processing system at the higher level of security until an encrypted

second authorization message is received. FIG. 1b, blocks 140 and 144 and the specification, page 6, lines 15-17.

(VI) Grounds of Rejection to be Reviewed on Appeal

Whether the rejection of claims 1-20 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,602,916 to Grube et al. in view of U.S. Patent No. 5,930,361 to Hayashi et al. is proper.

(VII) Argument

In the Rejection mailed April 26, 2006, the Examiner asserts "Grube et al. fail to disclose the reception of a second indicator to proceed to a lower security level and preventing operation at the second level until the reception." Rejection mailed April 26, 2006, page 4. The Examiner further asserts that Hayashi et al. teach a second indicator in column 1, line 52 – column 2, line 7. Id.

Hayashi et al. do not teach any indicator in column 1, line 52 – column 2, line 7 let alone an indicator as presently claimed. What Hayashi et al. do teach in this section is different encryption keys for different set-top boxes. This does not translate, however, to each set-top box operating at a different level of security or encryption.

As stated in the present specification, different encryption algorithms provide different levels of security. Specification, page 1, lines 26-31. However, more complex encryption algorithms, and therefore higher security, is achieved at the expense of needing additional memory, processing power and cycle times. Id. There is nothing in

this section of Hayashi et al. that equates a different encryption key to a different level of encryption.

Applicant asserts Hayashi et al. most likely have only one encryption algorithm in the plurality of set-top boxes. Thus, as an example, set-top box A has encryption algorithm ENC and set-top box B has encryption algorithm ENC. Set-top box A has decryption key 1234 and set-top box B has decryption key 5678. Content is encrypted at a server in the network using a key, say 4321, related to decryption key 1234. This content is then broadcast to both set-top boxes A and B. Set-top box A uses decryption key 1234 in algorithm ENC to decrypt and provide the content to the user. Set-top box B can attempt to use decryption key 5678 in algorithm ENC to decrypt the content but it will be unable. The decryption key 5678 will not work to decrypt content encrypted using encryption key 4321. Thus, set-top boxes A and B are operating at the same level of security, but because they have different keys, the stated purpose of Hayashi et al. in column 1, line 52 – column 2, line 7 is met since only set-top box A can decrypt the content.

For at least these reasons, the Examiner's rejections should be reversed and the application allowed.

(VIII) Claims Appendix

A copy of the claims, as amended by the amendment filed herewith, is attached.

(IX) Evidence Appendix

No additional evidence is provided in an evidence appendix.

(X) Related Proceedings Appendix

No related proceedings are provided in a related proceedings appendix.

Respectfully submitted,

Xin Qiu et al.

___/Benjamin D. Driscoll/_____ __January 26, 2007__

Benjamin D. Driscoll
Reg. No. 41,571
Motorola, Inc.
101 Tournament Drive
Horsham, PA 19044
P (215) 323-1840
F (215) 323-1300

Date

CLAIMS APPENDIX

1. A method of providing varying levels of security in a data processing system, the method comprising:

receiving information from an outside source;

retrieving a first indicator form the received information that instructs the system to operate at a higher level of security;

receiving further information from said outside source;

retrieving a separate second indicator from said further information received from said outside source, the second indicator for instructing the system to operate at a lower level of security than the higher level of security instructed by the first indicator; and

preventing operation at the lower level of security until a decrease in security levels is indicated by said second indicator; while

continuing operation of said processing system.

2. The method of claim 1 wherein said receiving further information comprises:

receiving an encrypted message, said encrypted message comprising a Decreased-Security-Authorization-Code to authorize said decrease in security levels.

3. The method of claim 2 wherein said Decreased-Security-Authorization-Code authorizes a decrease in encryption/decryption levels.

4. The method of claim 2 wherein said Decreased-Security-Authorization-Code authorizes a decrease in authentication level.

5. The method of claim 2 wherein said Decreased-Security-Authorization-Code authorizes a decrease in authentication level and a decrease in encryption/decryption levels.

6. The method of claim 2 wherein said encrypted message further comprises a key for use in a decryption algorithm.

7. The method of claim 6 wherein said system stores a master key to decrypt messages comprising new decryption key values and further comprising:

using said master key stored at said system to decrypt said encrypted message.

8. The method of claim 1 and further comprising:

establishing a Security-Level-Status-Indicator at said system to indicate a level of security that is being implemented by the system.

9. The method of claim 8 wherein said Security-Level-Status-Indicator indicates a level of encryption/decryption that is being implemented by the system.

10. The method of claim 8 wherein said Security-Level-Status-Indicator indicates a level of authentication that is being implemented by the system.

11. The method of claim 8 wherein said Security-Level-Status-Indicator indicates a level of authentication and a level encryption/decryption that is being implemented by the system.

12. The method of claim 8 and further comprising:

configuring said Security_Level_Status_Indicator to indicate more than two security levels so as to allow said system to utilize more than two security levels.

13. The method of claim 1 and further comprising:

utilizing a cable head-end as said outside source; and

utilizing a set-top box in order to retrieve the first and second indicators from the information received from the cable head-end.

14. The method of claim 2 and further comprising using a Key Management Message to convey said Decreased Security Authorization Code.

15. The method of claim 14 wherein delivery of said Key Management Message is authenticated.

16. The method of claim 14 wherein delivery of said Key Management Message is protected against a replay attack.

17. The method of claim 14 wherein delivery of said Key Management Message is authenticated and protected against a replay attack.

18. The method of claim 1 wherein a lower level of security is non-public Key mode, wherein a higher level of security is a public Key mode, the method further comprising:

continuing operation of the system in the public Key mode until an encrypted predefined message is received by the system from the outside source.

19. The method of claim 18 wherein said system stores a master key to decrypt messages comprising new decryption key values and further comprising:

using said master key stored at said system to decrypt said encrypted message.

20. A method of providing a secure transition between security levels in a data processing system, the data processing system having at least a high level of security and a low level of security for operation, the method comprising:

using the system to receive information form an outside source;

operating the system at the high level of security in response to a first security message in the information from the outside source;

continuing operation of the system at the high level of security until an encrypted, second authorization message is received by the system from the outside source authorizing a switch to a different level of security, the second authorization message being separate from the first security message.